IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

PAUL CULBERTSON, KATHY NEAL, KELLY ALLISON-PICKERING, JESSICA HAIMAN, ALEXANDER CABOT, BRIANA JULIUS, NICHELLE NEWLAND, BERNADETTE NOLEN and ALEXANDRIA POLICHENA, *individually and on behalf of all others similarly situated*, Plaintiffs, v. DELOITTE CONSULTING LLP, Defendant.	**Case No.: 1:20-cv-3962-LJL (lead case)** ***Consolidated with*** **Case No.: 1:20-cv-4129-LJL** **Case No.: 1:20-cv-4077-LJL** **Case No.: 1:20-cv-4362-LJL** **Case No.: 1:20-cv-5070-LJL** **JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

Plaintiffs PAUL CULBERTSON, KATHY NEAL, KELLY ALLISON-PICKERING, JESSICA HAIMAN, ALEXANDER CABOT, BRIANA JULIUS, NICHELLE NEWLAND, BERNADETTE NOLEN and ALEXANDRIA POLICHENA (collectively "Plaintiffs"), bring this class action individually and on behalf of others similarly situated against Defendant Deloitte Consulting LLP ("Deloitte" or "Defendant") seeking damages and equitable relief as set forth below. All allegations made in this complaint are made based on information and belief and investigation of counsel, except those allegations that pertain to Plaintiffs, which are based on personal knowledge. Each allegation in this Complaint has evidentiary support, or alternatively, pursuant to Rule 11(b)(3) of the Federal Rules of Civil Procedure, is likely to have evidentiary support after a reasonable opportunity for further investigation or discovery.

NATURE OF THE ACTION

1. Businesses that collect and store sensitive information about their customers have a duty to safeguard that information and ensure it remains private. This responsibility is essential where a business keeps and stores its customers' highly personal information, such as their names, email addresses, phone numbers, social security numbers, and/or bank account and/or routing information. Deloitte is one of those businesses.

2. In the wake of the COVID-19 pandemic and as part of the federal government's Pandemic Unemployment Assistance ("PUA") program, Deloitte formed contracts with various state agencies—including including the Ohio Department of Job and Family Services ("ODJFS"), the Illinois Department of Employment Security ("IDES"), and the Colorado Department of Labor and Employment ("CDLE")—to help those states administer the PUA program by designing, building, and maintaining web-based portals through which individuals may apply for unemployment benefits and communicate with state agencies.

3. Deloitte failed to take reasonable and adequate measures to secure the personally identifiable information ("PII") of Plaintiffs, their dependents, and similarly situated individuals (the Class Members, as defined below), in the course of designing, building, and maintaining computerized unemployment systems for multiple state agencies.

4. In May 2020, ODJFS, IDES, and CDLE publicly confirmed that Deloitte's web-portal similarly exposed the PII of applicants in their states.

5. Because of Deloitte's failure to exercise due care, members of the public were able to access unemployment applicants' PII, including social security numbers. As a result, Plaintiff and the Class Members have been injured through the loss of control of their PII, the need to spend

time to take appropriate steps to mitigate their injury, and the heightened and imminent risk of identity theft or fraud.

PARTIES

6. Plaintiff PAUL CULBERTSON ("Culbertson") is an adult who resides in and is a citizen of Akron, Ohio. Plaintiff Culbertson applied for unemployment benefits on April 26, 2020 through the PUA web-portal created and maintained by Deloitte for Ohio residents. Culbertson's PII was left publicly accessible. On or about May 20, 2020, Culbertson received correspondence from the ODJFS confirming the breach, and noting that his name, social security number, and street address associated with his PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit A.) As a result of Culbertson's data being exposed in this data breach, Culbertson has spent approximately three hours reviewing his bank statements, credit card statements, and credit history. He spent approximately one hour travelling to and spending time at his bank to gather and review bank statements. He also made three phone calls to the ODJFS seeking assistance regarding the breach, but he spent approximately 30 minutes waiting on hold and was unable to connect with a representative. He continues to monitor his financial statements and credit history for abnormal activity.

7. Plaintiff KATHY NEAL ("Neal") is an adult who resides in and is a citizen of Streamwood, Illinois. In May 2020, Neal applied for unemployment benefits through the PUA web-portal created and maintained by Deloitte for Illinois residents. Neal's PII was left publicly accessible. On May 21, 2020, Neal received correspondence from Deloitte confirming the breach, and noting that her name, social security number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit B.) As a result of Neal's data being exposed in this data breach, credit inquiries were made in Neal's name to open accounts

that she did not authorize. By way of example, Neal received notice of credit inquiries in Neal's name without her consent with Westlake Financial Services (on May 22, 2020) and with FingerHut. As a result of this fraudulent activity, Neal's credit score dropped drastically, and she spent time filing disputes with Equifax, TransUnion and Experian. Neal subsequently received an email from Experian that there was fraudulent activity with regard to her email account.

8. Plaintiff KELLEY ALLISON-PICKERING ("Allison-Pickering") is an adult who resides in and is a citizen of Parker, Colorado. Allison-Pickering applied for unemployment benefits on April 21, 2020 through the PUA web-portal created and maintained by Deloitte for Colorado residents. Allison-Pickering's PII was left publicly accessible. On or about May 18, 2020, Allison-Pickering received correspondence from the CDLE confirming the breach, and noting that her name, social security number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit C.) As a result of Allison-Pickering's data being exposed in this data breach, Allison-Pickering has spent a substantial amount of time reviewing her online banking records, credit card statements, and credit reports for fraudulent activity. Allison-Pickering has also experienced suspicious activity since the breach. Allison-Pickering's husband received a letter in the mail stating that an unknown loan application had been denied because his social security number could not be verified.

9. Plaintiff JESSICA HAIMAN ("Haiman") is an adult who resides in and is a citizen of Aurora, Illinois. On March 28, 2020, Haiman applied for unemployment benefits through the PUA web-portal created and maintained by Deloitte for Illinois residents. Haiman's PII was left publicly accessible. On or about June 17, 2020 Haiman received notice about the data breach from IDES. As a result of Haiman's data being exposed in this data breach, another bank account was opened in her name, resulting in the diversion of one of her unemployment payments to this

fraudulently constructed direct deposit account. As a result of her PII being stolen in this data breach, Haiman has spent over 50 hours making numerous calls to IDES attempting to recover the missing unemployment payment, filling out and filing a police report, reviewing transactions and adding protection to her bank account, and drafting and submitting an affidavit for a subpoena to the bank.

10. Plaintiff ALEXANDER CABOT ("Cabot") is an adult who resides in and is a citizen of Chicago, Illinois. Cabot applied for unemployment benefits on May 11, 2020 through the PUA web-portal created and maintained by Deloitte for Illinois residents. Cabot's PII was left publicly accessible. On or about May 21, 2020, Cabot received correspondence from the IDES confirming the breach, and noting that his name, social security number, and street address associated with his PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit D.) As a result of Cabot's data being exposed, Cabot has made dozens of telephone calls, emails, and faxes to the IDES, governor's office, and state representatives seeking assistance regarding the breach. Cabot has also experienced suspicious activities since the breach. On two occasions, Cabot received telephone calls about the processing an unknown auto loan. When Cabot called the number back, he received a message that the mailbox was no longer receiving calls. Cabot has also paid to review his credit report, continued to pay for a credit monitoring service, and spent a substantial amount of time reviewing bank statements for fraudulent activity.

11. Plaintiff BRIANA JULIUS ("Julius") is an adult who resides in and is a citizen of Lebanon, Illinois. Julius applied for unemployment benefits on or about May 12, 2020 through the PUA web-portal created and maintained by Deloitte for Illinois residents. Julius' PII, and that of her dependent minor son, were left publicly accessible. On May 21, 2020, Julius received correspondence the from IDES confirming the breach, and noting that her name, social security

number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit E.) As a result of Julius's data being exposed in this data breach, Julius has expended time and suffered loss of productivity from taking time to address and attempt to protect herself and her son from potential identity theft and fraud. For example, after receiving notice of the data breach, Julius incurred a fraudulent charge on her bank account from California. Julius' bank notified her of the suspicious activity by a phone call. Julius confirmed that she did not make the charge and that the charge was indeed fraudulent. The bank immediately closed her debit card in an attempt to foreclose any additional fraudulent charges. To date, however, Julius is still waiting for her new debit card and has been without debit card access to her bank account. Julius has spent more than five hours responding to the breach, including reviewing bank statements and reviewing her bank account online. Julius is also distressed that her young son's identity has been stolen and is concerned that his credit will be destroyed before he can even use it. As a result, Julius is in the process of responding to her son's identity theft, including taking time to speak with her auto insurance agent who revealed that Plaintiff's son's PII has been stolen. As a result of this recent revelation, Julius has spent a substantial number of hours checking her son's credit reports, filing a police report, and contacting the credit reporting agencies.

12. Plaintiff NICHELLE NEWLAND ("Newland") is an adult who resides in and is a citizen of Chillicothe, Ohio. Newland applied for unemployment benefits on May 12, 2020 through the PUA web-portal created and maintained by Deloitte for Ohio residents. Newland's PII was left publicly accessible. On or about May 20, 2020, Newland received correspondence from the ODJFS confirming the breach, and noting that her name, social security number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit F.) As a result of Newland's PII being exposed in this data breach, Newland was informed

on May 29, 2020 via email from Netspend that her Netspend card—which was the account in which her PUA benefits totaling $6,000.00 were deposited—was reported as stolen by an unidentified third party. Upon contacting Netspend on May 29, 2020 after receiving the email, Newland was informed that Netspend put a block on her account depriving Newland of the $6,000.00. On May 30, 2020, Newland received a text message from Netspend informing her that a transfer of $1,500.00 was made from her Netspend account to a Netspend account of an unidentified third party. After receiving this text message, Newland contacted Netspend by telephone on May 30, 2020. During this call, Newland was informed by a Netspend customer service agent that an unidentified third party accessed Newland's Netspend account online and changed the associated email address, telephone number, and password. Newland was able to change her Netspend password with the assistance of the Netspend customer service agent. After concluding the call and changing her password, Newland accessed her Netspend account on May 30, 2020 to stop an attempted transfer of $1,000.00 via Western Union from her Netspend account which she did not authorize, and close her Netspend account. Thereafter, Newland has been in repeated contact with ODJFS to try to gain access to her PUA funds. Newland estimates she has expended more than 30 hours of her time responding to the data breach to date.

13. Plaintiff BERNADETTE NOLEN ("Nolen") is an adult who resides in and is a citizen of Niles, Ohio. At the time of the application of benefits and all events related to the breach, Nolen lived in Mineral Ridge, Ohio. Nolen applied for unemployment benefits on May 13, 2020 through the PUA web-portal created and maintained by Deloitte for Ohio residents. Nolen's PII was left publicly accessible. On or about May 20, 2020, Nolen received correspondence from the ODJFS confirming the breach, and noting that her name, social security number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as

Exhibit G.) As a result of Nolen's data being exposed in this data breach, Nolen received a text message on May 23, 2020 from Netspend—which was the account in which her PUA benefits totaling $8,200.00 were deposited—that an unidentified third party had reported her Netspend card as stolen. After receiving the text message, Nolen spoke over the telephone with a customer service representative of Netspend who informed Nolen that her account was locked and her card—which she had in her possession and was her only means to readily access her much-needed PUA funds—was now canceled. Nolen was informed during this same telephone call that Netspend would be sending her a new card which could take at least one week. Within four hours of that May 23, 2020 telephone call, Nolen received an email from Netspend notifying her that Netspend had transferred $1,400.00 from her now-locked account to another unidentified Netspend account which Nolen did not open. Upon receiving this email, Nolen called Netspend and during the ninety minute call with a customer service representative Nolen was informed that (1) Netspend had opened a fraud investigation into her account, and (2) Netspend had three (not one) open accounts associated with Nolen. Following this telephone call, Nolen received an email from Western Union notifying her that $935.00 was wired from her Netspend account to an unidentified third party. Nolen called Western Union, but she could not stop the money transfer, as she did not have the reference number for the wire transfer. On May 24, 2020, Nolen contacted Netspend again by telephone, as she was notified that an unknown third party was attempting to order new cards associated with Nolen's Netspend account. In addition to the financial issues with Netspend and Western Union, Nolen was notified in late May 2020 that her phone number was transferred from her account with Boost Mobile to Metro PCS without her authorization, which forced Nolen to obtain new cellular service with Boost Mobile. Nolen filed a police report detailing all of this activity with the Weathersfield,

Ohio Police Department. During the time that Nolen was deprived of her PUA funds, Nolen fell behind on her rent payments and utility payments.

14. Plaintiff ALEXANDRIA POLICHENA ("Polichena") is an adult who resides in and is a citizen of Garrettsville, Ohio. Polichena applied for benefits on May 13, 2020 through the PUA web-portal created and maintained by Deloitte for Ohio residents. Polichena's PII was left publicly accessible. On or about May 20, 2020, Polichena received correspondence from the ODJFS confirming the breach, and noting that her name, social security number, and street address associated with her PUA claim had been compromised. (A copy of this email is attached hereto as Exhibit H.) After receiving this email, Polichena signed up for Lifelock on May 21, 2020, as Polichena was concerned about unauthorized use of her PII. Polichena's Lifelock subscription costs her $21.99 per month. Polichena also spent time reviewing her bank statements and credit reports from Experian, Equifax, and TransUnion since the breach, and has closed her back accounts and reopened new accounts as a result of the data breach (a process that took multiple trips to the bank and took several hours to accomplish).

15. Defendant DELOITTE CONSULTING LLP is a limited liability partnership organized under the laws of Delaware and registered to operate in New York State. Its headquarters and principal place of business is located in this District at 30 Rockefeller Plaza, New York, NY 10112.

16. In May 2020, officials from ODJFS, IDES, and CDL publicly confirmed that their computerized unemployment systems designed, built and maintained by Deloitte allowed public access to applicants' and their dependents' PII, including social security numbers, thereby exposing sensitive private data of an unknown number of people who had recently filed for unemployment benefits to unauthorized persons. Upon information and belief, Plaintiffs believe

the number of unemployment applicants and their dependents whose PII was exposed numbers in the hundreds of thousands.

JURISDICTION AND VENUE

17. The jurisdiction of this Court is founded upon 28 U.S.C. § 1332(d) (Class Action Fairness Act) in that this is a putative class action with more than 100 class members, more than $5 million in controversy, and the requisite diversity of citizenship.

18. Venue is appropriate pursuant to 28 U.S.C. § 1391. A substantial portion of the events and conduct giving rise to the violations alleged in this Complaint occurred in this District.

19. This Court has personal jurisdiction over Defendant because it has continuous and systematic contacts with this forum, maintains its corporate headquarters in this District, and the events giving rise to this matter arose out of those contacts.

STATEMENT OF COMMON FACTS

Deloitte's Administration of the PUA Program

20. Pandemic Unemployment Assistance is a federal program that expands unemployment insurance eligibility to self-employed workers, freelancers, independent contractors, and part-time workers impacted by the coronavirus pandemic in 2020. PUA is one of the programs established by the Coronavirus Aid, Relief, and Economic Security ("CARES") Act, a $2 trillion coronavirus emergency stimulus package that President Trump signed into law on March 27, 2020. The CARES Act expands states' ability to provide unemployment insurance to many workers affected by COVID-19, including people who would not otherwise be eligible for unemployment benefits.

21. Unemployment benefits are provided and administered by state governments. Some state governments—including those of Ohio, Illinois, and Colorado—contract with private

companies to provide unemployment insurance solutions such as claims services, wage determinations, benefit payments control, reporting services, administrative services, and document management services.[1]

22. Deloitte is a private company that provides public sector labor and employment services to states, including unemployment insurance solutions.

23. The governments of Ohio, Illinois, and Colorado contracted with Deloitte to design, build, and maintain the processing system required to administer the PUA program.

24. The system was built to collect all information needed for individuals to apply for PUA benefits, including sensitive PII such as names, addresses, and social security numbers of applicants and their dependents.

25. Deloitte knew that individuals, like Plaintiffs and absent Class Members, who applied for PUA benefits through its web-portals entrusted it with sensitive PII, and that safeguarding such information was vitally important.

26. The web-portals Deloitte designed for Ohio, Illinois, and Colorado were each activated on or around May 11, 2020.

The Value of Personal Identifying Information

27. It is well known that PII, and financial account information in particular, is an invaluable commodity and a frequent target of hackers.

28. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.[2]

---

[1] Deloitte, *Public Sector Labor and Employment services | uFACTS*, https://www2.deloitte.com/us/en/pages/public-sector/solutions/unemployment-insurance-services.html (last visited July 23, 2020).

[2] Javelin Strategy & Research, *Identity Fraud Hits All Time High With 16.7 Million U.S. Victims in 2017, According to New Javelin Strategy & Research Study* (Feb. 6, 2018), https://www.javelinstrategy.com/press-release/identity-fraud-hits-all-time-high-167-million-us-victims-2017-according-new-javelin (last visited July 23, 2020).

29. Consumers place a high value not only on their PII, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical reactions.[3]

30. Consumers are particularly concerned with protecting the privacy of their financial account information and social security numbers, which are the "secret sauce" that is "as good as your DNA to hackers."[4] There are long-term consequences to data breach victims whose social security numbers are taken and used by hackers. Even if they know their social security numbers have been accessed, Plaintiffs and Class Members cannot obtain new numbers unless they become a victim of social security number misuse. Even then, the Social Security Administration has warned that "a new number probably won't solve all [] problems … and won't guarantee … a fresh start."[5]

31. The PII of minors (like the dependents of many Class Members, including Julius's son, can be used to receive illicit gains through methods such as credit card fraud with newly created accounts. The fact that a minor's social security numbers has not yet been used for financial purposes actually makes it more valued by hackers rather than less. The "blank slate" credit file of a child is much less limited than the potentially low credit score of an adult. Social security numbers that have never been used for financial purposes are uniquely valuable as thieves can pair

[3] Identity Theft Resource Center, *Identity Theft: The Aftermath 2017*, https://www.ftc.gov/system/files/documents/public_comments/2017/10/00004-141444.pdf (last visited July 23, 2020).

[4] Cameron Huddleston, *How to Protect Your Kids From the Anthem Data Breach*, Kiplinger, (Feb. 10, 2015), https://www.kiplinger.com/article/credit/T048-C011-S001-how-to-protect-your-kids-from-the-anthem-data-brea.html (last visited July 23, 2020).

[5] Social Security Admin., *Identity Theft and Your Social Security Number*, at 6-7, https://www.ssa.gov/pubs/EN-05-10064.pdf (last visited July 23, 2020).

them with any name and birthdate. After that happens, thieves can open illicit credit cards or even sign up for government benefits.[6]

Industry Standards for Data Security

32. As an accounting organization with an acute interest in maintaining the confidentiality of its clients' information, Defendant is well aware of the numerous data breaches that have occurred throughout the United States and its responsibility for safeguarding users' PII.

33. Deloitte represents to its customers that it possesses robust security features to protect PII. Deloitte assures Plaintiffs and Class Members that it "use[s] a range of physical, electronic and managerial measures to ensure that we keep your personal information secure, accurate and up to date" and that "[s]afeguarding confidential information is core to the services Deloitte member firms provide. Deloitte is committed to protecting confidential and personal data including that of Deloitte clients and third parties."[7]

34. Deloitte also promotes its ability to protect PII through its Global Confidentiality and Privacy Office which purportedly "helps foster a culture across Deloitte that emphasizes the importance of protecting confidential and personal data … sets guidelines, develops procedures, provides consultation and training, and assesses the effectiveness of controls relating to confidentiality and privacy."[8]

35. Deloitte further represents that its Global Cybersecurity Office "works with the Deloitte Global Confidentiality and Privacy Office, as well as Deloitte confidentiality, privacy and

[6] Richard Power, "Child Identity Theft: New Evidence Indicates Identity Thieves are Targeting Children for Unused Social Security Numbers," Carnegie Mellon CyLab, https://www.cylab.cmu.edu/_files/pdfs/reports/2011/child-identity-theft.pdf (last visited July 23, 2020).

[7] https://www2.deloitte.com/global/en/legal/privacy.html (last accessed July 21, 2020).

[8] https://www2.deloitte.com/global/en/pages/about-deloitte/articles/information-security-privacy-confidentiality.html (last accessed July 21, 2020).

cybersecurity professionals around the world to execute an aggressive strategy designed to … [i]mplement and sustain leading practice technology safeguards to protect confidential and personal data … and [r]educe the risk of unauthorized exposure of confidential or personal data."[9]

36. In light of the numerous high-profile data breaches targeting companies like Target, Neiman Marcus, eBay, Anthem, and Equifax, Defendant is, or reasonably should have been, aware of the importance of safeguarding PII, as well as of the foreseeable consequences of its systems being breached.

37. Security standards commonly accepted among businesses that store PII using the internet include, without limitation:

a. Maintaining a secure firewall configuration;

b. Monitoring for suspicious or irregular traffic to servers;

c. Monitoring for suspicious credentials used to access servers;

d. Monitoring for suspicious or irregular activity by known users;

e. Monitoring for suspicious or unknown users;

f. Monitoring for suspicious or irregular server requests;

g. Monitoring for server requests for PII;

h. Monitoring for server requests from VPNs; and

i. Monitoring for server requests from Tor exit nodes.

[9] *Id.*

38. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[10] and protection of PII[11] which includes basic security standards applicable to all types of businesses.

39. The FTC recommends that businesses:

a. Identify all connections to the computers where you store sensitive information.

b. Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks.

c. Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business.

d. Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine.

e. Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks

[10] Start with Security: A Guide for Business, FTC (June 2015), https://www.ftc.gov/system/files/ documents/plain-language/pdf0205-startwithsecurity.pdf (last visited July 23, 2020).

[11] Protecting Personal Information: A Guide for Business, FTC (Oct. 2016), https://www.ftc.gov/ system/files/documents/plain-language/pdf-0136_proteting personalinformation.pdf (last visited July 23, 2020).

f. Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet.

g. Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically.

h. Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day.

i. Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

40. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as

an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[12]

41. Because Deloitte was entrusted with applicants' PII, it had, and has, a duty to applicants to keep their PII secure.

42. Applicants, such as Plaintiffs and the Class, reasonably expect that when they provide PII to a company, the company will safeguard their PII.

43. Nonetheless, Defendant failed to upgrade and maintain its data security systems in a meaningful way so as to prevent the data breach. Had Defendant properly maintained its systems and adequately protected them, it could have prevented the data breach.

44. Despite lacking appropriate safeguards to protect unemployment applicants' PII, the web-portal designed by Deloitte and used by at least Ohio, Illinois, and Colorado in the administration of the PUA program was activated on or around May 11, 2020.

The Data Breach

45. On May 15, 2020, Illinois State Representative Terri Bryant sent a letter to Illinois Governor Pritzker notifying him that a constituent "stumbled upon" a spreadsheet on the IDES portal containing PII of "thousands of employment applicants"—including names, addresses, social security numbers, and unemployment claim ID numbers.[13]

46. On May 17, 2020, officials from IDES confirmed that IDES was aware of a software "glitch" in the new PUA system designed and maintained by Deloitte that made "some

[12] Federal Trade Commission, *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (last visited July 15, 2020).

[13] https://repbryant.com/2020/05/16/rep-bryant-demands-governor-answer-questions-involving-potential-massive-ides-unemployment-applicant-data-breach (last visited July 23, 2020).

private information publicly available for a short time and worked to immediately remedy the situation."[14]

47. On May 18, 2020, officials from CDLE confirmed that it too experienced a "data access issue" with the new PUA system, which allowed strangers to view applicants' PII.[15] The CDLE assured, however, that "[o]ur vendor partner Deloitte worked swiftly once the unauthorized access was identified and fixed the issue within one hour."[16]

48. On May 20, 2020, ODJFS notified PUA program claimants by email that a security vulnerability in the PUA system designed and maintained by Deloitte allowed third party access to their names, social security number, and home address.

49. Plaintiffs each became aware of the data breach upon receipt of notice from their state's agency.

50. As a result of being notified of the data breach, Plaintiffs have been forced to take multiple precautionary steps to protect themselves and their property in an effort to avoid becoming a victim of identity fraud. These steps include, for example, reviewing bank statements, credit card statements and credit histories, attempting to recover missing unemployment payments, filling out and filing police reports, reviewing transactions and adding protection to bank accounts, calling the various state departments of employment security, and enrolling in credit monitoring services. Plaintiffs have also experienced suspicious activity subsequent to the data breach,

[14] https://patch.com/illinois/across-il/illinois-unemployment-website-glitch-leaks-personal-information (last visited July 23, 2020).

[15] https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html (last visited July 23, 2020).

[16] https://www.kktv.com/content/news/Colorado-Labor-Department-confirms-brief-data-exposure-for-pandemic-unemployment-claimants-570633261.html (last visited July 23, 2020).

including unrequested credit inquiries, and fraud activity on email accounts, bank accounts, and Netspend accounts.

51. Defendant itself acknowledged the imminent harm caused by the data breach, as it is offering 12 months of free credit monitoring to all PUA unemployment applicants in the affected states. This credit monitoring is insufficient to protect Plaintiffs as there is often a substantial time lag between when harm occurs and when it is discovered.[17] For example, according to a 2017 study, "the amount of fraud committed based on data breach data that is 2-6 years old ha[d] increased by nearly 400% over the last 4 years."[18]

52. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard the PII described above.

53. Defendant's substandard security practices were a direct and proximate cause of the massive data breach compromising the PII of hundreds of thousands of Americans.

54. Defendant failed to prevent the data breach because it did not adhere to commonly accepted security standards and failed to detect that its databases were subject to a security breach.

55. As a direct and proximate result of Defendant's actions and omissions in failing to protect Plaintiffs' PII, Plaintiffs and Class Members have been damaged.

56. Plaintiffs and Class Members have been placed at a substantial risk of harm in the form of credit fraud or identity theft and have incurred and will likely incur additional damages in order to prevent and mitigate credit fraud or identity theft. The information exposed in the data

[17] *See* Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," at 29, U.S. Government Accountability Office, June 2007, available at https:/www.gao.gov/new.items/d07737.pdf (last visited July 23, 2020).

[18] Brian Stack, "Here's How Much Your Personal Information is Selling for on the Dark Web," Experian (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web (last visited July 22, 2020).

breach is, by its very nature, the information necessary to obtain unemployment benefits, apply for and obtain lines of credit, and myriad financially-related activities.

57. In addition to the irreparable damage that may result from the theft of PII, identity theft victims must spend numerous hours and their own money repairing the impact to their credit. After conducting a study, the Department of Justice's Bureau of Justice Statistics found that identity theft victims "reported spending an average of about 7 hours clearing up the issues" and resolving the consequences of fraud in 2014.[19]

58. In addition to fraudulent charges and damage to their credit, Plaintiffs and Class Members will spend substantial time and expense (a) monitoring their accounts to identify fraudulent or suspicious charges; (b) cancelling and reissuing cards; (c) purchasing credit monitoring and identity theft prevention services; (d) attempting to withdraw funds linked to compromised, frozen accounts; (e) removing withdrawal and purchase limits on compromised accounts; (f) communicating with financial institutions to dispute fraudulent charges; (g) resetting automatic billing instructions; (h) freezing and unfreezing credit bureau account information; (i) cancelling and re-setting automatic payments as necessary; and (j) paying late fees and declined payment penalties as a result of failed automatic payments.

59. Additionally, Plaintiffs and Class Members have suffered or are at increased risk of suffering from, *inter alia*, the loss of the opportunity to control how their PII is used, the diminution in the value and/or use of their PII entrusted to Defendant, and loss of privacy.

[19] U.S. Department of Justice, *Victims of Identity Theft, 2014* (Revised November 13, 2017), available at http://www.bjs.gov/content/pub/pdf/vit14.pdf (last visited July 15, 2020).

CLASS ALLEGATIONS

60. Plaintiffs bring this Complaint on behalf of themselves and the following Classes:[20]

> The Nationwide Class: All persons in the United States whose PII was compromised or exposed as a result of the PUA portal data breach.
>
> The Ohio Class: All persons in the State of Ohio whose PII was compromised or exposed as a result of the PUA portal data breach.
>
> The Illinois Class: All persons in the State of Illinois whose PII was compromised or exposed as a result of the PUA portal data breach.
>
> The Colorado Class: All persons in the State of Colorado whose PII was compromised or exposed as a result of the PUA portal data breach.

61. The Class definition specifically excludes: (a) any persons or other entities currently related to or affiliated with Defendant; (b) any Judge presiding over this action and members of his or her family, members of their judicial staff, and any Judge sitting in the presiding court system who may hear an appeal of any judgment entered; and (c) all persons who properly execute and file a timely request for exclusion from the Class.

62. Class-wide adjudication of Plaintiffs' claims is appropriate because Plaintiffs can prove the elements of their claims on a class-wide basis using the same evidence as would be used to prove those elements in individual actions asserting the same claims.

63. *Numerosity*: The Class Members are so numerous that joinder of individual claims is impracticable. Since the COVID-19 pandemic, approximately 38.6 million U.S. residents have filed for unemployment. Although the precise number is not yet known to Plaintiffs, Plaintiffs

[20] Plaintiffs reserve the right to amend the Class definitions and to add subclasses as necessary.

reasonably approximate that the number of Class Members is in the hundreds of thousands.[21] The Class Members can be readily identified through Defendant's records.

64. *Commonality*: There are significant questions of fact and law common to the Class Members. These issues include but are not limited to:

a. Whether Defendant owed a duty or duties to Plaintiffs and Class Members to exercise due care in collecting, storing, safeguarding, and obtaining their PII;

b. Whether Defendant breached that duty or those duties;

c. Whether Defendant failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records to protect against known and anticipated threats to security;

d. Whether the security provided by Defendant was satisfactory to protect customer information as compared to industry standards;

e. Whether Defendant misrepresented or failed to provide adequate information to customers regarding the type of security practices used;

f. Whether Defendant knew or should have known that it did not employ reasonable measures to keep Plaintiffs' and Class Members' PII secure and prevent loss or misuse of that PII;

g. Whether Defendant acted negligently in connection with the monitoring and protecting of Plaintiffs' and Class Members' PII;

h. Whether Defendant's conduct was intentional, willful, or negligent;

[21] *See, e.g.*, https://www.nbcnews.com/business/economy/unemployment-claims-state-see-how-covid-19-has-destroyed-job-n1183686 (total unemployment claims since March 14, 2020: 407,861 in Colorado; 1,039,231 in Illinois; and 1,219,870 in Ohio)(last accessed May 21, 2020).

i. Whether Defendant violated any and all statutes and/or common law listed herein;

j. Whether Classes Members suffered damages as a result of Defendant's conduct, omissions, or misrepresentations; and

k. Whether Class Members are entitled to injunctive, declarative, and monetary relief as a result of Defendant's conduct.

65. *Typicality*: Plaintiffs' claims are typical of the claims of the Class. Plaintiffs and all Class Members have been adversely affected and damaged in that Defendant failed to adequately protect their PII to the detriment of Plaintiffs and the Class.

66. *Adequacy of Representation*: Plaintiffs will fairly and adequately represent the Class because they have the Class Members' best interests in mind, their individual claims are co-extensive with those of the Class, and they are represented by qualified counsel experienced in class action litigation of this nature.

67. *Superiority*: A class action is superior to other available methods for the fair and efficient adjudication of these claims because individual joinder of the claims of all Class Members is impracticable. Many Class Members are without the financial resources necessary to pursue this matter. Even if some Class Members could afford to litigate their claims separately, such a result would be unduly burdensome to the courts in which the individualized cases would proceed. Individual litigation increases the time and expense of resolving a common dispute concerning Defendant's actions toward an entire group of individuals. Class action procedures allow for far fewer management difficulties in matters of this type and provide the unique benefits of unitary adjudication, economies of scale, and comprehensive supervision over the entire controversy by a single judge in a single court.

68. The Class may be certified pursuant to Rule 23(b)(2) of the Federal Rules of Civil Procedure because Defendant has acted on grounds generally applicable to the Class, thereby making final injunctive relief and corresponding declaratory relief appropriate with respect to the claims raised by the Class.

69. The Class may also be certified pursuant to Rule 23(b)(3) of the Federal Rules of Civil Procedure because questions of law and fact common to Class Members will predominate over questions affecting individual members, and a class action is superior to other methods for fairly and efficiently adjudicating the controversy and causes of action described in this Complaint.

70. Particular issues under Rule 23(c)(4) are appropriate for certification because such claims present particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein.

COUNT I

NEGLIGENCE

(Brought on behalf of the Nationwide Class, or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

71. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

72. Defendant owed a duty of care to Plaintiffs and Class Members to use reasonable means to secure and safeguard the entrusted PII, to prevent its unauthorized access and disclosure, to guard it from theft, and to detect any attempted or actual breach of its systems. These common law duties existed because Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices. In fact, not only was it foreseeable that Plaintiffs and Class Members would be harmed by the failure to protect their PII because hackers routinely attempt to

steal such information and use it for nefarious purposes, Defendant knew that it was more likely than not Plaintiffs and other Class Members would be harmed by such exposure of their PII.

73. Defendant's duties to use reasonable security measures also arose as a result of the special relationship that existed between Defendant, on the one hand, and Plaintiffs and Class Members, on the other hand. The special relationship arose because Plaintiffs and Class Members entrusted Defendant with their PII as part of process for applying for unemployment insurance. Defendant alone could have ensured that its data security systems and practices were sufficient to prevent or minimize the data breach.

74. Defendant's duties to use reasonable data security measures also arose under Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect PII. Various FTC publications and data security breach orders further form the basis of Defendant's duties. In addition, individual states have enacted statutes based upon the FTC Act that also created a duty.

75. Defendant breached the aforementioned duties when it failed to use security practices that would protect the PII provided to it by Plaintiffs and Class Members, thus resulting in unauthorized third party access to the Plaintiffs' and Class Members' PII.

76. Defendant further breached the aforementioned duties by failing to design, adopt, implement, control, manage, monitor, update, and audit its processes, controls, policies, procedures, and protocols to comply with the applicable laws and safeguard and protect Plaintiffs' and Class Members' PII within its possession, custody, and control.

77. As a direct and proximate cause of failing to use appropriate security practices, Plaintiffs' and Class Members' PII was disseminated and made available to unauthorized third parties.

78. Defendant admitted that Plaintiffs' and Class Members' PII was wrongfully disclosed as a result of the breach.

79. The breach caused direct and substantial damages to Plaintiffs and Class Members, as well as the possibility of future and imminent harm through the dissemination of their PII and the greatly enhanced risk of credit fraud or identity theft.

80. By engaging in the forgoing acts and omissions, Defendant committed the common law tort of negligence. For all the reasons stated above, Defendant's conduct was negligent and departed from reasonable standards of care including by, but not limited to: failing to adequately protect the PII; failing to conduct regular security audits; and failing to provide adequate and appropriate supervision of persons having access to Plaintiffs' and Class Members' PII.

81. But for Defendant's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, their PII would not have been compromised.

82. Neither Plaintiffs nor Class Members contributed to the breach or subsequent misuse of their PII as described in this Complaint. As a direct and proximate result of Defendant's actions and inactions, Plaintiffs and Class Members have been put at an increased risk of credit fraud or identity theft, and Defendant has an obligation to mitigate damages by providing adequate credit and identity monitoring services. Defendant is liable to Plaintiffs and Class Members for the reasonable costs of future credit and identity monitoring services for a reasonable period of time, substantially in excess of one year. Defendant is also liable to Plaintiffs and Class Members to the extent that they have directly sustained damages as a result of identity theft or other unauthorized

use of their PII, including the amount of time Plaintiffs and the Class Members have spent and will continue to spend as a result of Defendant's negligence. Defendant is also liable to Plaintiffs and Class Members to the extent their PII has been diminished in value because Plaintiffs and Class Members no longer control their PII and to whom it is disseminated.

COUNT II

NEGLIGENCE PER SE

(Brought on Behalf of the Nationwide Class, or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

83. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

84. Pursuant to the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security to safeguard the PII of Plaintiffs and Class Members.

85. The FTC Act prohibits "unfair . . . practices in or affecting commerce," which the FTC has interpreted to include businesses' failure to use reasonable measures to protect PII. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

86. Defendant solicited, gathered, and stored PII of Plaintiffs and the Class Members to facilitate transactions which affect commerce.

87. Defendant violated the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII of Plaintiffs and the Class Members and not complying with applicable industry standards, as described herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

88. Defendant's violation of the FTC Act (and similar state statutes) constitutes negligence per se.

89. Plaintiffs and the Class Members are within the class of persons that the FTC Act was intended to protect.

90. The harm that occurred as a result of the breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures caused the same harm as that suffered by Plaintiffs and the Class Members.

91. As a direct and proximate result of Defendant's negligence *per se*, Plaintiffs and the Class Members have suffered, and continue to suffer, damages arising from the breach as described above.

COUNT III

INVASION OF PRIVACY

(Brought on Behalf of the Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

92. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

93. Defendant invaded Plaintiffs' and the Class Members' right to privacy by allowing the unauthorized access to Plaintiffs' and Class Members' PII and by negligently maintaining the confidentiality of Plaintiffs' and Class Members' PII, as set forth above.

94. The intrusion was offensive and objectionable to Plaintiffs, the Class Members, and to a reasonable person of ordinary sensibilities in that Plaintiffs' and Class Members' PII was disclosed without prior written authorization of Plaintiffs and the Class.

95. The intrusion was into a place or thing which was private and is entitled to be private, in that Plaintiffs and the Class Members provided and disclosed their PII to Defendant privately with an intention that the PII would be kept confidential and protected from unauthorized disclosure. Plaintiffs and the Class Members were reasonable to believe that such information would be kept private and would not be disclosed without their written authorization.

96. As a direct and proximate result of Defendant's above acts, Plaintiffs' and the Class Members' PII was viewed, distributed, and used by persons without prior written authorization and Plaintiffs and the Class Members suffered damages as described herein.

97. Defendant is guilty of oppression, fraud, or malice by permitting the unauthorized disclosure of Plaintiffs' and the Class Members' PII with a willful and conscious disregard of Plaintiffs' and the Class Members' right to privacy.

98. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause Plaintiffs and the Class Members great and irreparable injury in that the PII maintained by Defendant can be viewed, printed, distributed, and used by unauthorized persons. Plaintiffs and Class Members have no adequate remedy at law for the injuries in that a judgment for the monetary damages will not end the invasion of privacy for Plaintiffs and the Class, and Defendant may freely treat Plaintiffs' and Class Members' PII with sub-standard and insufficient protections.

COUNT IV

UNJUST ENRICHMENT

(Brought on Behalf of the Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

99. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70 and plead this claim, to the extent necessary, in the alternative to their claims at law.

100. Plaintiffs and Class Members have an interest, both equitable and legal, in their PII that was conferred upon, collected by, and maintained by Defendant and that was ultimately compromised in the data breach.

101. Defendant, by way of its acts and omissions, knowingly and deliberately enriched itself by saving the costs it reasonably should have expended on security measures to secure Plaintiffs' and Class Members' PII.

102. Defendant also understood and appreciated that the PII pertaining to Plaintiffs and Class Members was private and confidential and its value depended upon Defendant maintaining the privacy and confidentiality of that PII.

103. Instead of providing for a reasonable level of security that would have prevented the breach—as is common practice among companies entrusted with such PII—Defendant instead consciously and opportunistically calculated to increase its own profits at the expense of Plaintiffs and Class Members. Nevertheless, Defendant continued to obtain the benefits conferred on it by Plaintiffs and Class Members. The benefits conferred upon, received, and enjoyed by Defendant were not conferred officiously or gratuitously, and it would be inequitable and unjust for Defendant to retain these benefits.

104. Plaintiffs and Class Members, on the other hand, suffered as a direct and proximate result. As a result of Defendant's decision to profit rather than provide requisite security, and the resulting breach disclosing Plaintiffs' and Class Members' PII, Plaintiffs and Class Members suffered and continue to suffer considerable injuries in the forms of, *inter alia,* attempted identity theft, time and expenses mitigating harms, diminished value of PII, loss of privacy, and increased risk of harm.

105. Thus, Defendant engaged in opportunistic conduct in spite of its duties to Plaintiffs and Class Members, wherein it profited from interference with Plaintiffs' and Class Members' legally protected interests. As such, it would be inequitable, unconscionable, and unlawful to permit Defendant to retain the benefits it derived as a consequence of its conduct.

106. Accordingly, Plaintiffs, on behalf of themselves and the Class, respectfully request that this Court award relief in the form of restitution or disgorgement in the amount of the benefit conferred on Defendant as a result of its wrongful conduct, including specifically, the amounts that Defendant should have spent to provide reasonable and adequate data security to protect Plaintiffs' and Class Members' PII, and/or compensatory damages.

COUNT V

BAILMENT

(Brought on Behalf of Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

107. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

108. Plaintiffs and Class Members provided, or authorized disclosure of, their PII to Defendant for the exclusive purpose of applying for unemployment benefits and using the associated portal.

109. In allowing their PII to be made available to Defendant, Plaintiffs and Class Members intended and understood that Defendant would adequately safeguard their PII.

110. For its own benefit, Defendant accepted possession of Plaintiffs' and Class Members' PII for the purpose of making available its own services.

111. By accepting possession of Plaintiffs' and Class Members' PII, Defendant understood that Plaintiffs and Class Members expected Defendant to adequately safeguard their

personal information. Accordingly, a bailment (or deposit) was established for the mutual benefit of the parties. During the bailment (or deposit), Defendant owed a duty to Plaintiffs and Class Members to exercise reasonable care, diligence, and prudence in protecting their personal information.

112. Defendant breached its duty of care by failing to take appropriate measures to safeguard and protect Plaintiffs' and Class Members' personal information, resulting in the unlawful and unauthorized access to and misuse of Plaintiffs' and Class Members' PII.

113. As a direct and proximate result of Defendant's breach of its duty, Plaintiffs and Class Members suffered consequential damages that were reasonably foreseeable to Defendant, including but not limited to the damages set forth above.

114. As a direct and proximate result of Defendant's breach of its duties, the personal information of Plaintiffs and Class Members entrusted, directly or indirectly, to Defendant during the bailment (or deposit) was damaged and its value diminished.

COUNT VI

BREACH OF CONTRACT

(Brought on Behalf of the Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

115. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

116. When Defendant and the various state governments entered into contracts to provide Plaintiffs and Class Members with benefits under the PUA program, they intended to directly provide financial and other benefits to Plaintiffs and Class Members. As a result, Defendant received taxpayer funds through the CARES Act and was required to be provided Plaintiffs' and Class Members' PII, which it was obligated to keep confidential. Accordingly,

Plaintiffs and Class Members were intended third-party beneficiaries under the contracts between the government and Defendant.

117. Defendant violated the contracts by failing to employ reasonable and adequate privacy practices and measures, leading to the disclosure of Plaintiffs' and Class Members' PII for purposes not required or permitted under the contracts or the law.

118. Plaintiffs and Class Members have been damaged by Defendant's breaches of its contracts with their state governments by incurring the harms and injuries described herein arising from the Data Breach now and in the future. Additionally, because Plaintiffs and Class Members continue to be third-party beneficiaries in the ongoing administration and distribution of benefits to them under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiffs and Class Members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII from unlawful exposure.

119. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and it is liable to Plaintiffs and Class Members for associated damages and specific performance.

COUNT VII

BREACH OF IMPLIED CONTRACT

(Brought on Behalf of the Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

120. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

121. Defendant invited applicants, including Plaintiffs and the Class Members, to use its portal in order to apply for unemployment benefits. As consideration for the benefits Defendants

were to administer, Plaintiffs and Class Members provided their PII to Defendant. When Plaintiffs and Class Members provided their PII to Defendant, they entered into implied contracts by which Defendant agreed to protect their PII and only use it solely to administer benefits. As part of the offer, Defendant would safeguard the PII using reasonable or industry-standard means.

122. Accordingly, Plaintiffs and the Class Members accepted Defendant's offer to administer benefits (for which Defendant was compensated by their state governments) and provided Defendant their PII by using the portal.

123. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant. However, Defendant breached the implied contracts by failing to safeguard Plaintiffs' and Class Members' PII.

124. The losses and damages Plaintiffs and Class Members sustained that are described herein were the direct and proximate result of Defendant's breaches of its implied contracts with them. Additionally, because Plaintiffs and Class Members continue to be parties to the ongoing administration and distribution of benefits under the contracts, and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiffs and Class Members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII from unlawful exposure.

125. Defendant's conduct as alleged herein also violated the implied covenant of good faith and fair dealing inherent in every contract, and it is liable to Plaintiffs and Class Members for associated damages and specific performance.

COUNT VIII

BREACH OF IMPLIED COVENANT OF GOOD FAITH AND FAIR DEALING

(Brought on Behalf of the Nationwide Class or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

126. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

127. As described above, Plaintiffs and Class Members were (1) third-party beneficiaries under the contracts between Defendant and their governments; and (2) were parties to an implied contract with Defendant when they provided their PII in order to obtain benefits.

128. Inherent in every contract is that implied covenant of good faith and fair dealing, which Defendant violated by failing to maintain reasonable data security protocols, leading to the disclosure of Plaintiffs and Class Members' PII for purposes not required or permitted under the contracts or applicable law.

129. The losses and damages Plaintiffs and Class Members sustained that are described herein and were the direct and proximate result of Defendant's breaches of the implied covenant of good faith and fair dealing. Additionally, because Plaintiffs and Class Members continue to be parties to the ongoing administration and distribution of benefits under the contracts (and as intended third-party beneficiaries of the contracts between Defendant and their governments), and because damages may not provide a complete remedy for the breaches alleged herein, Plaintiffs and Class Members are therefore entitled to specific performance of the contracts to ensure data security measures necessary to properly effectuate the contracts maintain the security of their PII from unlawful exposure.

COUNT IX

BREACH OF CONFIDENCE

(Brought on Behalf of the Nationwide Class, or, in the alternative, the Ohio Class, the Illinois Class and the Colorado Class)

130. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

131. As alleged above, Plaintiff and Class Members had agreements with Defendant, both express and implied, that required Defendant to keep their PI confidential.

132. Defendant breached that confidence by disclosing Plaintiffs' and Class Members' PI without their authorization and for unnecessary purposes.

133. As a result of the data breach, Plaintiff and Class Members suffered damages that were attributable to Defendant's failure to maintain confidence in their PII.

COUNT X

COLORADO CONSUMER PROTECTION ACT
Colo. Rev. Stat. §§ 6-1-101, et seq.

(Brought on behalf of the Colorado Class)

134. Plaintiff Allison-Pickering ("Plaintiff," for purposes of this Count), individually and on behalf of the Colorado Class, repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

135. Deloitte is a "person" as defined by Colo. Rev. Stat. § 6-1-102(6).

136. Plaintiff and Colorado Class Members are persons who were injured by Deloitte's engaging in deceptive trade practices in the course of its business.

137. Defendant engaged in deceptive trade practices in the course of its business, in violation of Colo. Rev. Stat. § 6-1-105(1), including by:

a. Knowingly or recklessly making a false representation as to the characteristics of products and services;

b. Representing that services are of a particular standard, quality, or grade, though Defendant knew or should have known that they were another;

c. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Colorado Class Members' PII, which was a direct and proximate cause of the data breach;

d. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the data breach;

e. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Colorado Class Members' PII, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Colorado Class Members' PII; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Colorado Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

138. Defendant's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Deloitte's data security and ability to protect the confidentiality of PII.

139. Deloitte intended to mislead Plaintiff and Colorado Class Members, as well as the state agencies with which it contracted, and induce them to rely on its misrepresentations and omissions.

140. Plaintiff and the Colorado Class Members acted reasonably in relying on Deloitte's misrepresentations and omissions, the truth of which they could not have discovered.

141. Deloitte acted intentionally, knowingly, and maliciously to violate Colorado's Consumer Protection Act, and recklessly disregarded Plaintiff and Colorado Class Members' rights.

142. As a direct and proximate result of Deloitte's deceptive trade practices, Plaintiff and Colorado Class Members suffered injuries to their legally protected interests, including their legally protected interest in the confidentiality and privacy of their PII.

143. Deloitte's deceptive trade practices significantly impact the public because it is providing services that are used by thousands of Colorado consumers to receive essential benefits.

144. Plaintiff and Colorado Class Members seek all monetary and non-monetary relief allowed by law, including the greater of: (a) actual damages, (b) $500, or (c) three times actual damages (for Deloitte's bad faith conduct); injunctive relief; and reasonable attorneys' fees and costs.

COUNT XI

ILLINOIS UNIFORM DECEPTIVE TRADE PRACTICES ACT, 815 IlCS §§ 510/1, et seq.

(On behalf of the Illinois Class)

145. Plaintiffs Neal, Haiman, Cabot and Julius ("Plaintiffs" for purposes of this Count), individually and on behalf of the Illinois Class, repeats and reaffirm Paragraphs 1-70, as if fully alleged herein.

146. Deloitte is a "person" as defined by 815 ILCS § 510/1(5).

147. Deloitte engaged in deceptive trade practices in the conduct of its business, in violation of 815 ILCS§ 510/2(a), including:

a. Representing that goods or services have characteristics that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade if they are of another;

c. Engaging in other conduct that creates a likelihood of confusion or misunderstanding;

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs and Illinois Class Members' PII, which was a direct and proximate cause of the data breach;

e. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures, which was a direct and proximate cause of the data breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the data breach;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Illinois Class Members' PII, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45;

i. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs and Illinois Class Members' PII; and

j. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs and Illinois Class Members' PII, including duties imposed by the FTC Act, 15 U.S.C. § 45.

148. Defendant's representations and omissions were material because they were likely to deceive reasonable persons about the adequacy of Deloitte's data security and ability to protect the confidentiality of PII.

149. The above unfair and deceptive practices and acts by Deloitte were immoral, unethical, oppressive, and unscrupulous. These acts caused substantial injury to Plaintiff and Illinois Class Members that they could not reasonably avoid; this substantial injury outweighed any benefits to the public or competition.

150. As a direct and proximate result of Deloitte's unfair, unlawful, and deceptive trade practices, Plaintiff and Illinois Class Members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, as described herein.

151. Plaintiff and Illinois Class Members seek all monetary and non-monetary relief allowed by law, including injunctive relief and reasonable attorney's fees.

COUNT XII

INJUNCTIVE RELIEF

(Brought on Behalf of the Nationwide Class)

152. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

153. Defendant's above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting security breach have caused (and will continue to cause) Plaintiffs and Class Members to suffer irreparable harm in the form of, *inter alia*, (i) identity theft and identity fraud, (ii) invasion of privacy, (iii) loss of the intrinsic value of their privacy and PII, (iv) breach of the confidentiality of their PII, (v) deprivation of the value of their PII, for which

there is a well- established national and international market, (vi) the financial and temporal cost of monitoring their credit, monitoring their financial accounts, and mitigating their damages, and (vii) the imminent, immediate, and continuing increased risk of ongoing identity theft and identity fraud. Such irreparable harm will not cease unless and until enjoined by this Court.

154. Plaintiffs and Class Members, therefore, are entitled to injunctive relief and other appropriate affirmative relief including, *inter alia*, an order compelling Defendant to (i) notify each person whose PII was exposed in the security breach, (ii) provide credit monitoring to each such person for a reasonable period of time, substantially in excess of one year, (iii) establish a fund (in an amount to be determined) to which such persons may apply for reimbursement of the time and out-of-pocket expenses they incurred to remediate identity theft and/or identity fraud (*i.e.*, data breach insurance), and (iv) discontinue its above-described wrongful actions, inaction, omissions, want of ordinary care, nondisclosures, and resulting security breach.

155. Plaintiffs and Class Members also are entitled to injunctive relief requiring Defendant to implement and maintain data security measures, policies, procedures, controls, protocols, and software and hardware systems, including, *inter alia*, (i) engaging third-party security auditors/penetration testers and internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's computer systems on a periodic basis, (ii) engaging third-party security auditors and internal personnel to run automated security monitoring, (iii) auditing, testing, and training its security personnel regarding any new or modified procedures, (iv) conducting regular database scanning and security checks, (v) regularly evaluating web applications for vulnerabilities to prevent web application threats, and (vi) periodically conducting internal training and education to inform internal data security personnel how to identify and contain data security lapses.

156. If an injunction is not issued, Plaintiffs and Class Members will suffer irreparable injury in the event Defendant commits another security lapse, the risk of which is real, immediate, and substantial.

157. The hardship to Plaintiffs and Class Members if an injunction does not issue exceeds the hardship to Defendant if an injunction is issued. Among other things, if Defendant suffers another massive security lapse, Plaintiffs and Class Members will likely again incur millions of dollars in damages. On the other hand, and setting aside the fact that Defendant has a pre-existing legal obligation to employ adequate data security measures, Defendant's cost to comply with the above-described injunction it is already required to implement is relatively minimal.

158. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another security lapse, thereby eliminating the damages, injury, and harm that would be suffered by Plaintiffs, Class Members, and the numerous future applicants whose confidential and sensitive PII would be compromised.

COUNT XIII

DECLARATORY RELIEF

(Brought on Behalf of the Nationwide Class)

159. Plaintiffs repeat and reaffirm, as if fully set forth, the allegations of paragraphs 1 through 70.

160. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.,* the Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

161. An actual controversy has arisen in the wake of the data breach regarding Defendant's present and prospective common law and other duties to reasonably safeguard PII and whether Defendant is currently maintaining data security measures adequate to protect Plaintiffs and Class Members from further data breaches that compromise their PII. Plaintiffs and Class Members remain at imminent risk that further compromises of their PII will occur in the future.

162. Pursuant to the Declaratory Judgment Act, 28 U.S.C. §2201, *et seq.,* Plaintiffs and Class Members request the Court to enter a judgment declaring, *inter alia*, (i) Defendant owed (and continues to owe) a legal duty to safeguard and protect Plaintiffs' and Class Members' PII, (ii) Defendant breached (and continues to breach) such legal duties by failing to safeguard and protect Plaintiffs' and Class Members' PII, and (iii) Defendant's breach of its legal duties directly and proximately caused the breach, and the resulting damages, injury, and harm suffered by Plaintiffs and Class Members.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, for themselves and Class Members, respectfully request that:

A. This action be certified as a class action;

B. Plaintiffs be designated Class Representatives; and

C. Plaintiffs' counsel be appointed as Class Counsel;

D. Judgment be awarded against Defendant, in Plaintiffs' favor for:

(i) compensatory and punitive damages in an amount to be determined by the trier of fact;

(ii) declaratory and injunctive relief (as set forth above);

(iii) attorneys' fees, litigation expenses, and costs of suit incurred through the trial and any appeals of this case;

(iv) pre- and post-judgment interest on any amounts awarded; and

(v) such other and further relief the Court deems just and proper.

JURY DEMAND

Plaintiffs, individually and on behalf of the Class Members, respectfully demand a trial by jury on all of their claims and causes of action so triable.

Dated: July 24, 2020

Respectfully submitted,

KAPLAN FOX & KILSHEIMER LLP

By: /s/ *Frederic S. Fox*
Frederic S. Fox

Frederic S. Fox (S.D.N.Y. Bar FF9102)
David A. Straite (S.D.N.Y. Bar DS0114)
850 Third Avenue
New York, NY 10022
Phone: (212) 687-1980
Fax: (212) 687-7714
ffox@kaplanfox.com
dstraite@kaplanfox.com

KAPLAN FOX & KILSHEIMER LLP
Laurence D. King (S.D.N.Y. Bar LK7190)
Matthew B. George*
1999 Harrison Street, Suite 1560
Oakland, California 94612
Phone: (415) 772-4700
Fax: (415) 772-4707
lking@kaplanfox.com
mgeorge@kaplanfox.com

GOLDENBERG SCHNEIDER, L.P.A.
Jeffrey S. Goldenberg (pro hac vice)
4445 Lake Forest Drive, Suite 490
Cincinnati, OH 45242
Phone: (513) 345-8297
Fax: (513) 345-8294
jgoldenberg@gs-legal.com

MORGAN & MORGAN
John A. Yanchunis (pro hac vice)
201 North Franklin Street, 7th Floor
Tampa, Florida 33602
Phone: (813) 275-5272
JYanchunis@ForThePeople.com

MORGAN & MORGAN
Amanda Peterson (Fed. Bar No. AP1797)
90 Broad Street, Suite 1011
New York, NY 10004
Phone: (212) 738-6299
apeterson@forthepeople.com

LEVIN SEDRAN & BERMAN, LLP
Charles E. Schaffer (*pro hac vice*)
510 Walnut Street – Suite 500
Philadelphia, PA 19106-3697
Phone: (215) 592-1500
cschaffer@lfsblaw.com

THE LYON FIRM, P.C.
Joseph M. Lyon (*pro hac vice*)
2754 Erie Ave
Cincinnati, Ohio 45208
Phone: (513) 381-2333
jlyon@thelyonfirm.com

MASON LIETZ & KLINGER LLP
Gary E. Mason (*pro hac vice*)
5101 Wisconsin Avenue, NW, Suite 305
Washington, D.C. 20016
Phone: (202) 640-1160
gmason@masonllp.com

TYCKO & ZAVAREEI LLP
Hassan A. Zavareei*
Katherine M. Aizpuru (Fed. Bar No. 5305990)
1828 L Street NW, Suite 1000
Washington, D.C. 20036
Phone: (202) 973-0900
Fax: (202) 973-0950
hzavareei@tzlegal.com
kaizpuru@tzlegal.com

PEARSON, SIMON & WARSHAW, LLP
Melissa S. Weiner*
800 LaSalle Avenue, Suite 2150
Minneapolis, Minnesota 55402
Phone: (612) 389-0600
Fax: (612) 389-0610
mweiner@pswlaw.com
jbourne@pswlaw.com

KOPELOWITZ OSTROW FERGUSON WEISELBERG GILBERT
Jeff Ostrow*
Jonathan M. Streisfeld*
1 West Las Olas Blvd. Suite 500
Fort Lauderdale, FL 33301
Phone: (954) 525-4100
Fax: (954) 525-4300
ostrow@kolawyers.com
streisfeld@kolawyers.com

ZIMMERMAN LAW OFFICES, P.C.
Thomas A. Zimmerman, Jr. (*pro hac vice*)
Sharon A. Harris*
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
Phone: (312) 440-0020
Fax: (312) 440-4180
tom@attorneyzim.com
sharon@attorneyzim.com

DANNLAW
Javier L. Merino (Fed. Bar. No. JM4291)
372 Kinderkamack Road, Suite 5
Westwood, NJ 07675
Phone: (201) 355-3440
Fax: (216) 373-0536
notices@dannlaw.com

DANNLAW
Marc E. Dann (*pro hac vice*)
Brian D. Flick*
PO Box 6031040
Cleveland, OH 44103
Phone: (216) 373-0539
Fax: (216) 373-0536
notices@dannlaw.com

CARLSON LYNCH LLP
Katrina Carroll*
Kyle A. Shamberg*
111 W. Washington Street, Suite 1240
Chicago, IL 60602
Phone: (312) 750-1265
kcarroll@carlsonlynch.com
kshamberg@carlsonlynch.com

FREED KANNER LONDON & MILLEN LLC
Jonathan M. Jagher*
Kimberly A. Justice *
923 Fayette Street
Conshohocken, PA 19428
Phone: (610) 234-6487
jjagher@fklmlaw.com
kjustice@fklmlaw.com

CONSUMER PROTECTION LEGAL, LLC
Tiffany Marko Yiatras (*pro hac vice*)
308 Hutchinson Road
Ellisville, Missouri 63011-2029
Phone: (314) 541-0317
tiffany@consumerprotectionlegal.com

LAW OFFICE OF FRANCIS J. "CASEY" FLYNN, JR.
Francis J. "Casey" Flynn, Jr.*
3518A Arsenal Street
Saint Louis, Missouri 63118
Phone: (314) 662-2836
casey@lawofficeflynn.com

Attorneys for Plaintiffs

**Pro Hac Vice* Forthcoming

CERTIFICATE OF SERVICE

I certify that a copy of the foregoing was filed electronically on July 24, 2020, via the Court Clerk's CM/ECF system, which will provide notice to all counsel of record.

/s/ *Frederic S. Fox*
Frederic S. Fox